

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 3 of 25

Amendment to the Claims

Please amend the claims as follows:

1. (Currently amended) A method for configuring a semiconductor chip ~~having an associated serial number~~, the method comprising:
selecting a private cryptographic key;
selecting a public cryptographic key, wherein the public cryptographic key and the private cryptographic key are not related by a ~~cryptographic~~ public/private key pair relationship; ~~and~~
embedding the private cryptographic key; ~~and the public cryptographic key, and the serial number~~ in a read-only memory on the semiconductor chip; ~~and~~
storing a second public cryptographic key associated with the private cryptographic key exclusively outside the semiconductor chip.
2. (Original) The method of claim 1 wherein the semiconductor chip provides interface processing at a client.
3. (Cancelled)
4. (Currently amended) The method of claim 1 further comprising:
storing the public cryptographic key in a database in association with ~~the a serial number~~ associated with the semiconductor chip.
5. (Original) The method of claim 1 wherein the private cryptographic key, and the public cryptographic key in the read-only memory are inaccessible to an input/output connection of the semiconductor chip.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed; April 12, 2001
Page 4 of 25

6. (Currently amended) An article of manufacture comprising:
a first read-only memory structure containing an embedded private cryptographic key, the embedded private cryptographic key being associated with a stored public cryptographic key stored exclusively outside the first read-only memory structure; and
a second read-only memory structure containing an embedded public cryptographic key, wherein the embedded public cryptographic key and the embedded private cryptographic key are not related by a cryptographic public/private key pair relationship.
7. (Original) The article of manufacture of claim 6 wherein the article of manufacture is a semiconductor chip.
8. (Original) The article of manufacture of claim 7 wherein the semiconductor chip is capable of providing interface processing at a client.
9. (Original) The article of manufacture of claim 8 wherein the first read-only memory structure and the second read-only memory structure are contained within a cryptographic unit of a CPU chip.
10. (Currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:
generating a client message at the client;
retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a cryptographic public/private key pair relationship, the embedded client private key being associated with a client public key stored exclusively outside the client;

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 5 of 25

encrypting the client message with the embedded server public key; and
sending the client message to the server.

11. (Previously presented) The method of claim 10 further comprising:
retrieving client authentication data;
retrieving the embedded client private key from a read-only memory structure in
an article of manufacture in the client;
encrypting the client authentication data with the embedded client private key;
and
storing the encrypted client authentication data in the client message.
12. (Original) The method of claim 11 further comprising:
retrieving an embedded client serial number from a read-only memory structure in
an article of manufacture in the client; and
storing a copy of the embedded client serial number in the client message.
13. (Currently amended) An apparatus for secure communication between a client
and a server in a data processing system, the apparatus comprising:
means for generating a client message at the client;
means for retrieving an embedded server public key from a read-only memory
structure in an article of manufacture in the client, the read-only memory structure having an
embedded client private key, the embedded server public key and the embedded client private
key not being related by a ~~cryptographic~~ public/private key pair relationship, the embedded client
private key being associated with a client public key stored exclusively outside the client;

May 15, 2006
Case No. AUS920010088JS1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 6 of 25

means for encrypting the client message with the embedded server public key;

and

means for sending the client message to the server.

14. (Previously presented) The apparatus of claim 13 further comprising:
means for retrieving client authentication data;
means for retrieving the embedded client private key from a read-only memory structure in an article of manufacture in the client;
means for encrypting the client authentication data with the embedded client private key; and
means for storing the encrypted client authentication data in the client message.

15. (Original) The apparatus of claim 14 further comprising:
means for retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and
means for storing a copy of the embedded client serial number in the client message.

16. (Currently amended) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:
instructions for generating a client message at the client;
instructions for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client, the read-only memory structure having an embedded client private key, the embedded server public key and the embedded client private key not being related by a ~~cryptographic~~ public/private key pair relationship, the

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 7 of 25

embedded client private key being associated with a client public key stored exclusively outside the client;

instructions for encrypting the client message with the embedded server public key; and instructions for sending the client message to the server.

17. (Previously presented) The computer program product of claim 16 further comprising:

instructions for retrieving client authentication data;

instructions for retrieving the embedded client private key from a read-only memory structure in an article of manufacture in the client;

instructions for encrypting the client authentication data with the embedded client private key; and

instructions for storing the encrypted client authentication data in the client message.

18. (Original) The computer program product of claim 17 further comprising:

instructions for retrieving an embedded client serial number from a read-only memory structure in an article of manufacture in the client; and

instructions for storing a copy of the embedded client serial number in the client message.

19. (Previously presented) A method for secure communication between a client and a server in a data processing system, the method comprising:

generating a server message at the server;

retrieving information that was requested by the client;

storing the retrieved information in the server message;

May 15, 2006
Case No. AUS920010088(JS1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 8 of 25

retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client;

encrypting the server message with the client public key; and
sending the server message to the client.

20. (Previously presented) The method of claim 19 further comprising:
retrieving server authentication data;
retrieving a server private key;
encrypting the server authentication data with the server private key; and
storing the encrypted server authentication data in the server message.

21. (Previously presented) An apparatus for secure communication between a client and a server in a data processing system, the apparatus comprising:
means for generating a server message at the server;
means for retrieving information that was requested by the client;
means for storing the retrieved information in the server message;
means for retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client;
means for encrypting the server message with the client public key; and
means for sending the server message to the client.

22. (Original) The apparatus of claim 21 further comprising:
means for retrieving server authentication data;
means for retrieving a server private key;

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 9 of 25

means for encrypting the server authentication data with the server private key;
and
means for storing the encrypted server authentication data in the server message.

23. (Previously presented) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:
instructions for generating a server message at the server;
instructions for retrieving information that was requested by the client;
instructions for storing the retrieved information in the server message;
instructions for retrieving a client public key, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client, and the client public key is stored exclusively outside the client;
instructions for encrypting the server message with the client public key; and
instructions for sending the server message to the client.

24. (Original) The computer program product of claim 23 further comprising:
instructions for retrieving server authentication data;
instructions for retrieving a server private key;
instructions for encrypting the server authentication data with the server private key; and
instructions for storing the encrypted server authentication data in the server message.

25. (Currently amended) A method for secure communication between a client and a server in a data processing system, the method comprising:
receiving a client message from the client;

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 10 of 25

retrieving a server private key;
decrypting the client message with the server private key;
retrieving a client serial number from the decrypted client message; and
retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client;

wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a ~~cryptographic~~ public/private key pair relationship.

26. (Original) The method of claim 25 further comprising:

retrieving encrypted client authentication data from the client message;
decrypting the client authentication data with the retrieved client public key; and
verifying the decrypted client authentication data.

27. (Currently amended) An apparatus for secure communication between a client and a server in a data processing system, the apparatus comprising:

means for receiving a client message from the client;
means for retrieving a server private key;
means for decrypting the client message with the server private key;
means for retrieving a client serial number from the decrypted client message; and
means for retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client;

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 11 of 25

wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a ~~cryptographic~~ public/private key pair relationship.

28. (Original) The apparatus of claim 27 further comprising:
means for retrieving encrypted client authentication data from the client message;
means for decrypting the client authentication data with the retrieved client public key; and
means for verifying the decrypted client authentication data.

29. (Currently amended) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:

instructions for receiving a client message from the client;
instructions for retrieving a server private key;
instructions for decrypting the client message with the server private key;
instructions for retrieving a client serial number from the decrypted client message; and
instructions for retrieving a client public key that is associatively stored with the retrieved client serial number, wherein the client public key corresponds to an embedded client private key in a read-only memory structure in an article of manufacture in the client and is stored exclusively outside the client;

wherein the read-only memory structure has an embedded server public key, the embedded server public key and the embedded client private key not being related by a ~~cryptographic~~ public/private key pair relationship.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 12 of 25

30. (Original) The computer program product of claim 29 further comprising:
instructions for retrieving encrypted client authentication data from the client
message;
instructions for decrypting the client authentication data with the retrieved client
public key; and
instructions for verifying the decrypted client authentication data.
31. (Previously presented) A method for secure communication between a client and
a server in a data processing system, the method comprising:
receiving a server message from the server;
retrieving an embedded client private key from a read-only memory structure in
an article of manufacture in the client, the embedded client private key being associated with a
client public key stored exclusively outside the client; and
decrypting the server message with the embedded client private key.
32. (Original) The method of claim 31 further comprising:
retrieving encrypted server authentication data from the server message;
retrieving an embedded server public key from a read-only memory structure in an article
of manufacture in the client; and
decrypting the server authentication data with the embedded server public key;
and
verifying the decrypted server authentication data.
33. (Original) The method of claim 32 further comprising:
retrieving requested information from the server message; and
in response to a determination that the decrypted server authentication data was
verified, processing the requested information.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed; April 12, 2001
Page 13 of 25

34. (Previously presented) An apparatus for secure communication between a client and a server in a data processing system, the apparatus comprising:

means for receiving a server message from the server;

means for retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key stored exclusively outside the client; and

means for decrypting the server message with the embedded client private key.

35. (Original) The apparatus of claim 34 further comprising:

means for retrieving encrypted server authentication data from the server message;

means for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client; and

means for decrypting the server authentication data with the embedded server public key; and

means for verifying the decrypted server authentication data.

36. (Original) The apparatus of claim 35 further comprising:

means for retrieving requested information from the server message; and

means for processing the requested information in response to a determination that the decrypted server authentication data was verified.

May 15, 2006
Case No. AUS920010088US1 (9000/108)
Serial No. 09/833,342
Filed: April 12, 2001
Page 14 of 25

37. (Previously presented) A computer program product in a computer-readable medium for use in a data processing system for secure communication between a client and a server, the computer program product comprising:

- instructions for receiving a server message from the server;
- instructions for retrieving an embedded client private key from a read-only memory structure in an article of manufacture in the client, the embedded client private key being associated with a client public key stored exclusively outside the client; and
- instructions for decrypting the server message with the embedded client private key.

38. (Original) The computer program product of claim 37 further comprising:
instructions for retrieving encrypted server authentication data from the server message;

- instructions for retrieving an embedded server public key from a read-only memory structure in an article of manufacture in the client; and
- instructions for decrypting the server authentication data with the embedded server public key; and
- instructions for verifying the decrypted server authentication data.

39. (Original) The computer program product of claim 38 further comprising:
instructions for retrieving requested information from the server message; and
instructions for processing the requested information in response to a determination that the decrypted server authentication data was verified.

40. (New) The method of claim 1 wherein the embedding step further comprises the embedding of a serial number associated with the semiconductor chip.